CLAIMS

1. A system for external monitoring of networked digital file sharing to track predetermined data content, the system comprising:

at least one surveillance element for distribution over said network, said surveillance elements comprising:

search functionality for nodewise searching of said networked digital file sharing and

identification functionality associated with said search functionality for identification of said predetermined data content, therewith to determine whether a given file sharing system is distributing said predetermined data content.

2. A system according to claim 1, said search functionality being operable to carry out searching at a low level of a network protocol.

3. A system according to claim 1, said search functionality being operable to carry out searching at a high level of a network protocol.

4. A system according to claim 1, said search functionality being operable to carry out said searching at an application level.

5. A system according to claim 1, wherein said surveillance element is a first surveillance element and said search functionality comprises functionality for operating search features of said networked digital file sharing.

6. A system according to claim 5, wherein said identification functionality comprises use of a signature of said predetermined content.

7. A system according to claim 6, wherein said signature comprises a title of said predetermined content.

8. A system according to claim 6, wherein said signature comprises a derivative of a title of said predetermined content.

9. A system according to claim 6, wherein said signature comprises a statistical processing result carried out on said content.

10. A system according to claim 6, wherein said signature comprises a signal processing result carried out on said content.

11. A system according to claim 6, wherein said signature comprises a description of said content.

12. A system according to claim 6, wherein said signature is a derivative of the description of said content.

13. A system according to claim 1, wherein said surveillance element is a second surveillance element and comprises interception functionality for

intercepting data transport on said network, and wherein said identification functionality is associated with said interception functionality for finding an indication of said data content within said intercepted data transport.

14. A system according to claim 5, wherein said identification functionality comprises a signature of said predetermined content for comparison with data of said intercepted message to determine whether said message contains said evidence of said data content.

15. A system according to claim 14, wherein said content comprises alphanumeric data and said signature is a derivation of said alphanumeric data.

16. A system according to claim 14, wherein said content comprises binary data and said signature comprises a derivation of said binary data.

17. A system according to claim 16, said derivation being a hash function of said binary data.

18. A system according to claim 16, said derivation being function of metadata of said content.

19. A system according to claim 14, wherein said signature comprises a title of the said data content.

20. A system according to claim 9, wherein said signature comprises a derivative of the title of the said data content.

21. A system according to claim 9, wherein said signature comprises a statistical processing result carried out on said content.

22. A system according to claim 9, wherein said signature comprises a signal processing result carried out on said content.

23. A system according to claim 9, wherein said signature comprises a description of said content.

24. A system according to claim 9, wherein said signature comprises a derivative of the description of said content.

25. A system according to claim 1, wherein said surveillance element further comprises input/output functionality for receiving commands from said system and sending results of said search.

26. A system according to claim 25, further comprising a co-ordination element for interacting with said distributed input/output functionality to control deployment of said surveillance elements over said network and to monitor results from a plurality of said surveillance elements.

27. A system according to claim 26, said co-ordination element further being operable to interact with reaction elements by providing said reaction elements with details of locations of said predetermined content obtained from said surveillance elements, thereby to prompt said reaction elements to react against said locations.

28. A system according to claim 1, wherein said file sharing comprises a document exchange system and said surveillance element further comprises functionality for representing itself as a host server for said system, thereby to obtain data of documents on said system for said search functionality.

29. A system according to claim 1, comprising:

at least two first surveillance elements, each first surveillance element comprising functionality for operating search features of said networked digital file sharing.

at least two second surveillance elements, each said second surveillance element comprising interception functionality for intercepting messaging on said network, and wherein said identification functionality is associated with said interception functionality for identifying evidences of said data content within said intercepted messages, and

at least one control element for deploying said surveillance elements around said network and obtaining search results from said surveillance elements.

30. A system according to claim 22, wherein said surveillance element is a first surveillance element and said search functionality comprises functionality for operating search features of said networked digital file sharing.

31. A system according to claim 23, wherein said identification input functionality is operable to receive input from a comparator associated with a signature holder for holding a signature of said predetermined content, said comparator being operable to compare said content against said signature thereby to indicate to said input functionality the presence of said content.

32. A system according to claim 24, wherein said signature comprises a title of said predetermined content.

33. A system according to claim 24, wherein said signature is a derivative of a title of said predetermined content.

34. A system according to claim 24, wherein said signature comprises a statistical processing result carried out on said content.

35. A system according to claim 24, wherein said signature comprises a signal processing result carried out on said content.

36. A system according to claim 24, wherein said signature comprises a description of said content.

37. A system according to claim 24, wherein said signature comprises a derivative of a description of said content.

38. A system according to claim 22, wherein said surveillance element is a second surveillance element and comprises interception functionality for intercepting messaging on said network, and wherein said identification functionality is associated with said interception functionality for identifying evidences of said data content within said intercepted messages.

39. A system according to claim 23, wherein said search functionality further comprises input/output functionality for receiving commands from said system and sending results of said search.

40. A system according to claim 31, further comprising a co-ordination element for interacting with said distributed input/output functionality to control deployment of said surveillance elements over said network and to monitor results from a plurality of said surveillance elements, said co-ordination element further being operable to interact with said attack elements by providing said attack elements with details of locations of said predetermined content obtained from said surveillance elements, thereby to prompt said attack elements to attack said locations.

41. A system according to claim 22, wherein said file sharing comprises a document exchange system and said surveillance element further comprises functionality for representing itself as a host server for said system, thereby to obtain data of said file sharing for said search functionality.

42. A system according to claim 33, said identification functionality being operable to identify items in said document exchange system comprising said predetermined content.

43. A system according to claim 42, said attack element comprising functionality to send to said system a delete command to delete said item throughout said system.

44. A system according to claim 22, wherein said attack element comprises repetitive output functionality for repeatedly sending response requests to said file sharing system.

45. A system according to claim 36, wherein said response request comprises a download request.

46. A system according to claim 37, operable to co-ordinate response requests between a plurality of attack elements distributed over said network.

47. A system according to claim 38, operable to co-ordinate download requests between a plurality of said attack elements distributed over said network.

48. A system according to claim 22, wherein said surveillance agent

is a third surveillance element, comprising network protocol scan functionality operable to intercept and analyze network communication items of a predetermined network traffic, thereby to find protected content in transport.

49. A system according to claim 22, comprising at least one attack element wherein said attack functionality is operable to utilize features of said file sharing in said attack

50. A system according to claim 22, comprising at least one attack element wherein said attack functionality comprises transport interference functionality for interfering with messaging over said network.

51. A system according to claim 42, wherein said transport interference functionality comprises exchange functionality for exchanging said predetermined message content in said messaging with other message content.

52. A system according to claim 31, comprising:

at least two first surveillance elements, each first search element comprising functionality for operating search features of said networked digital file sharing.

at least two second surveillance elements, each said second surveillance element comprising interception functionality for intercepting messaging on said network, and wherein said identification functionality is associated with said interception functionality for identifying evidences of said data content within said intercepted messages,

at least two of said attack elements, and

at least one control element for distributing said surveillance and attack elements around said network, obtaining surveillance results from said surveillance elements, and coordinating activity of said attack elements to carry out a coordinated multiple point attack on said file sharing system.

53. A system for external monitoring and control of networked digital file sharing to track predetermined data content and limit distribution thereof, the system comprising:

at least one surveillance element for distribution over said network, said surveillance element comprising:

surveillance functionality for searching said digital file sharing and

identification input functionality associated with said search functionality for receiving an indication of the presence of said predetermined content, and

at least one attack element, comprising:

input functionality for receiving identification data of a file sharing system found to be distributing said predetermined content, and

attack functionality for applying an attack to said file sharing system to reduce said file sharing system's ability to distribute said predetermined data content. .

54. A network external content distribution control system comprising

network content identification functionality for identifying predetermined content

distributed over a digital file sharing network, said network comprising a plurality of nodes, and

network attack functionality for applying an attack over said digital file sharing network, said attack being directable to reduce the ability of the network to distribute said identified content.

55. A system according to claim 54, at least one of said nodes being identified to have said predetermined content, and at least one of said nodes being identified as a distribution node of said network, said attack being directable at said distribution node.

56. A network external content distribution control system comprising at least one surveillance unit for exploring a network to determine at least one of a presence and a distribution pattern of predetermined content and for reporting said determination for remote analysis.

57. A network scanning element for use in a network external content distribution control system, said scanning element being operable to scan at least a portion of a network suspected of distributing predetermined content by connecting to available ports in the network portion, via said port connections to determine the presence of network nodes participating in said distribution.

58. A method of externally scanning a distributed network comprising a plurality of nodes, to search for predetermined content available for distribution from said nodes, the method comprising:

distributing at least one surveillance element to said network, said surveillance element comprising:

search functionality for nodewise searching of said networked digital file sharing and

identification functionality associated with said search functionality for identification of said predetermined data content, therewith to determine whether a given file sharing system is distributing said predetermined data content.